PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: WO 99/38063

(43) International Publication Date: 29 July 1999 (29.07.99)

(21) International Application Number: PCT/US99/01614

(22) International Filing Date: 26 January 1999 (26.01.99)

(30) Priority Data:

60/072,714	27 January 1998 (27.01.98)	US
09/106,304	29 June 1998 (29.06.98)	US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PAL01-521, Palo Alto, CA 94303 (US).

(72) Inventors: RADUCHEL, William, J.; 3111 Alexis Drive, Palo Alto, CA 94304 (US). GUPTA, Abhay; 231 Dixon Landing Road, #121, Milpitas, CA 95035 (US). WILSON, Yvonne; 915 San Pierre Way, Mountain View, CA 94043 (US).

(74) Agents: GARRETT, Arthur, S.; Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315 (US) et al.

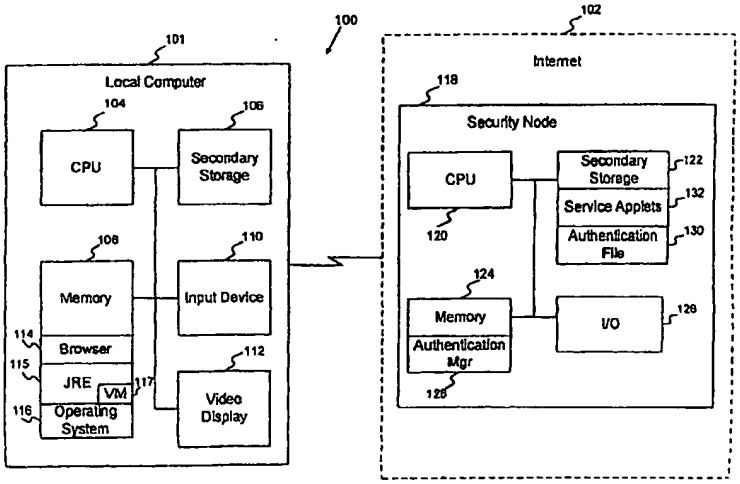
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: NETWORK-BASED AUTHENTICATION OF A COMPUTER USER



(57) Abstract

A network-based authentication scheme is provided that performs authentication in a centralized manner for the stand-alone computers of a particular organization. Since authentication is centralized, the individual computers do not need to store authentication information, and control over all of the computers rests in a single location, enabling the system administrator to manage access and utilization of the computers from this location. The network-based authentication scheme includes an authentication manager, remotely located with respect to a local computer, that performs authentication for the local computer. The authentication manager receives login information from the local computer, verifies this information against an authentication file, and returns indications of the services on the local computer that the user is able to utilize. The local computer receives these indications and displays icons representing the services available to that user. The user may then select an icon, causing an applet to be downloaded from the authentication manager onto the local computer to facilitate the user's utilization of the corresponding service.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

NETWORK-BASED AUTHENTICATION OF A COMPUTER USER

Related Application

The following identified U.S. provisional patent application is relied upon and is incorporated by reference in this application: Provisional U.S. Patent Application No. 60/072,714, entitled, "Integration of a Stand-Alone Computer into a Network-Based Computing Environment," filed on January 27, 1998.

Field of the Invention

The present invention relates generally to data processing systems and, more particularly, to network-based authentication of a computer user.

Background of the Invention

Conventional stand-alone computers typically perform their own authentication, a process known as local authentication. A "stand-alone computer" refers to a computer that is fully functional without having to connect to another device. Since the computer is fully functional, it has a processor, input/output capabilities, and an operating system with a file system. Conventional stand-alone computers perform local authentication by authenticating a user when the user attempts to log into the computer and then, based upon the outcome of the authentication, by either allowing or inhibiting the user from using the services of the computer. The term "services" refers to functionality provided by the computer system, such as access to the file system, e-mail system, or calendaring system.

Performing local authentication has its drawbacks in certain environments. Specifically, performing local authentication in a large organization is difficult because a large organization typically has many users using many interconnected computers, and multiple users may utilize the same computer. In such an organization, the computers are interconnected via a network, such as a local-area network, wide-area network, or the Internet, and it would be very difficult

to enable each computer to authenticate any user that may want to use it. Another drawback is that a system administrator is typically unable to control access and use of each of the individual computers unless he configures each one individually. Such an effort is very time consuming and is not practical for large organizations. It is therefore desirable to improve the authentication scheme of computers that are interconnected by a network.

Brief Description of the Drawings

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an implementation of the invention and, together with the description, serve to explain the advantages and principles of the invention. In the drawings,

Fig. 1 depicts a data processing system suitable for use with methods and systems consistent with the present invention;

Fig. 2 depicts a flow chart of the steps performed during login to the local computer depicted in Fig. 1;

Fig. 3 depicts a login screen presented by the browser depicted in Fig. 1;

Fig. 4 depicts a flow chart of the steps performed by the authentication manager depicted in Fig. 1;

Fig. 5 depicts the browser of Fig. 1 displaying icons representing available services to the user; and

Fig. 6 depicts the browser of Fig. 1 displaying icons representing all the services available on the local computer.

Summary of the Invention

A network-based authentication scheme is provided that performs authentication in a centralized manner for the interconnected stand-alone computers of a particular organization. Since authentication is centralized, the individual computers do not need to store authentication information, and authentication control over all of the computers rests in a single location, enabling a system administrator to manage access and utilization of the computers from this location.

In accordance with methods and systems consistent with the present invention, an authentication manager, remotely located with respect to a local computer, performs authentication for the local computer. The authentication manager receives login information from the local computer, verifies this information against an authentication file, and returns indications of the local computer services that the user is able to utilize. The local computer receives these indications and displays icons representing the services available to that user. The user may then select an icon, causing an applet to be downloaded from the authentication manager (or another server) onto the local computer to facilitate the user's utilization of the corresponding service.

In accordance with methods consistent with the present invention, a method for performing authentication in a computer system with services is provided. According to this method, an identification of a user is received, the identification is sent to a remote location to determine which among the services the user is authorized to use, and code is received that facilitates use of at least one of the services, where the user has been authorized to use this service.

In accordance with methods consistent with the present invention, a method for performing authentication in a data processing system having an authentication server and a computer system with services is provided. The authentication server performs the method by

receiving an identification of the user of the computer system, by determining which among the services the user is authorized to use, and by sending to the computer system code that facilitates use of the services that the user is authorized to use.

In accordance with systems consistent with the present invention, a data processing system with services and a user is provided. This data processing system includes a security node and a computer system. The security node includes an authentication manager configured to receive an identification of the user, configured to authenticate the user based on the identification, and configured to return code that facilitates use of the services when the user has been authenticated. The computer system includes a browser configured to receive the user identification, configured to send the user identification to the authentication manager, configured to receive the code, and configured to invoke the code to facilitate the use of the services by the user when the user has been authenticated.

Detailed Description

Methods and systems consistent with the present invention provide an improved authentication scheme. This authentication scheme centralizes authentication-related processing in an authentication manager so that the network administrator may easily control both the access and the use of each computer on the administrator's network.

Overview

In accordance with methods and systems consistent with the present invention, a computer system may perform a number of services. Some of these services are local to the computer in that they are performed by the operating system. Other services are downloaded from the authentication manager (or another server) upon authentication (e.g., application

programs like e-mail and calendaring). In the situation where the services are provided by the operating system, the user is unable to utilize the services until authentication is successfully completed and the user is granted access to those services. To gain access to one of these services, code must be downloaded from the authentication manager, in the form of an applet, that provides a user interface to the service. For example, if the service is a file system, the applet provides a command line or other graphical user interface so that the user could enter commands to manipulate the file system. An "applet" comprises code that usually runs in another program like a browser. In the situation where the services are remote, the user is unable to utilize the services because the code that performs the services are applets downloaded from the authentication manager (or other server) only after successful authentication.

In accordance with methods and systems consistent with the present invention, when a stand-alone computer starts up, the user is unable to utilize any of the services of the computer until an authentication process is successfully completed. To perform authentication, the computer runs a browser with an applet that displays a logon screen to the user, who then enters log-in information (e.g., username and password). Upon receiving this log-in information, the applet transfers it to an authentication manager, remotely located somewhere in the network, that determines whether the user should be able to use all the available services of the computer or only a limited subset of the available services. If the user is authenticated, the authentication manager enables the user to use additional services of the computer, such as access to files, change calendar information, and access to applications that the user is otherwise authorized to use. To do so, the authentication manager downloads to the browser an indication of the services the user is able to use. The browser then displays icons indicating each of these services, and the user may select the icons, causing applets that either perform these services or provide access to

these services to be downloaded to the browser and run, thus enabling the user to utilize the services.

If the user is not authenticated, the authentication manager enables him to only utilize a subset of the services provided by the computer, such as calendaring and e-mail; he is unable to utilize other services provided by the computer such as accessing the local file system. To enable the user to use this subset, the authentication manager downloads an indication of the services the user is allowed to use, and the browser displays icons which, when selected, cause applets to be downloaded that facilitate use of these services.

Implementation Details

Figure 1 depicts a data processing system 100 suitable for use with methods and systems consistent with the present invention. Data processing system 100 comprises local computer 101 connected to the Internet 102. Local computer 101 is a stand-alone computer and hence is fully functional, containing central processing unit (CPU) 104, secondary storage device 106, memory 108, input device 110, and video display 112. Memory 108 contains browser 114, Java™ Runtime Environment 115, and operating system 116. The browser 114 provides access to web pages on the Internet 102 and runs on the Java Runtime Environment 115. An example of a suitable browser is the HotJava Browser available from Sun Microsystems of Palo Alto, CA. The Java Runtime Environment 115 includes Java™ Virtual Machine 117, which acts like an abstract computing machine, receiving instructions in the form of bytecodes and interpreting the bytecodes by dynamically converting them into a format suitable for execution on the processor and by executing them. The Java Virtual Machine is described in greater detail in Lindholm and Yellin, The Java Virtual Machine Specification, Addison-Wesley (1997), which is incorporated herein by reference.

Internet 102 contains security node 118 with CPU 120, secondary storage device 122, memory 124, and at least one I/O device 126. Secondary storage device 122 contains authentication file 130, storing the data against which users are authenticated, and service applets 132, facilitating use of various computer services when downloaded to browser 114. Authentication file 130 contains the user name and password for authenticated users. Alternatively, one skilled in the art will appreciate that the authentication file 130 may contain information for performing authentication with digital token cards, such as enigma cards or information for performing authentication using digital certificates (such as x.509).

Service applets 132 facilitate use of a particular service when downloaded and run in browser 114 of local computer 101. For example, one service applet may be a file system applet providing a command-line user interface or graphical user interface that allows a user to manipulate the file system. Such an applet may be constructed using well-known user interface techniques to interact with the user and may use the Java™ class libraries to manipulate the file system. In this case, the applet is "signed" or authenticated such that it can provide access to the file system. The Java class libraries are described in greater detail in Chan and Lee, The Java Class Libraries: An Annotated Reference, Addison-Wesley (1997), which is incorporated herein by reference. Other examples of service applets include an e-mail applet and a calendar applet that perform either well-known e-mail functionality or time-management functionality, respectfully.

Although data processing system 100 depicts one computer being authenticated by the authentication manager, one skilled in the art will appreciate that the authentication manager may be used to perform authentication for many computers. Additionally, although aspects of the present invention are described as being stored in memory, one skilled in the art will appreciate that these aspects can also be stored on or read from other types of computer-readable media,

such as secondary storage devices, like hard disks, floppy disks, or CD-ROM; a carrier wave from the Internet; or other forms of RAM or ROM. Furthermore, although local computer 101 is depicted as being connected to the Internet, one skilled in the art will appreciate that, instead of the Internet, the local computer may be connected to other networks like an Intranet or other local-area or wide-area networks. Sun, Sun Microsystems, the Sun Logo, Java and Java-based trademarks are trademarks or registered trademarks of Sun Microsystems Inc. in the United States and other countries.

Methods and systems consistent with the present invention are described in greater detail with reference to Figure 2, which depicts a flowchart of the steps performed at start-up time of local computer 101. When the local computer is initially started, a small portion of the operating system is loaded (step 202). In this step, the minimum code necessary to run authentication is loaded, including VM 117 as well as the minimum components of the operating system necessary to load and run a web browser; it does not include a command interpreter or file capabilities.

Next, the browser is loaded and run (step 204). As shown in Figure 3, when running the browser, the user is initially presented with a screen 300 having a login dialog box 302 into which the user can enter their username and password. This screen is displayed by an applet, stored with the browser, that performs authentication by communicating with the authentication manager. In an alternative embodiment, the user enters a user name and is prompted with a challenge number which is entered into a digital token card and the resulting password is entered into the system. In another alternative embodiment, the local computer includes a smartcard reader and the user inserts a smartcard into the reader. However received, the authentication information, including the username and password, is sent by the browser to the authentication manager using the well-known HyperText Transfer Protocol (HTTPS), and using the well-known Secure Socket Layer (step 206).

The authentication manager receives the log-in information and uses it to authenticate the user, as shown in Figure 4. Although various embodiments of the authentication manager may vary and could be configurable, in one implementation, the authentication manager receives a log-in request containing a user name and password (step 402 in Figure 4). After receiving this information, the authentication manager authenticates the user by accessing the authentication file to determine if the user name and password are contained in it (step 404) and returns a token that identifies the services that the user may use (step 406). Additionally, this token may contain a profile of the user's access rights, and when the token is returned to the local computer, it would be included in all further requests from the local computer.

Returning to Figure 2, the local computer receives the authentication results from the authentication manager and determines if the user was authenticated (step 208). If authentication fails (i.e., the returned token indicates only a limited number of services), the user is allowed only to perform actions considered non-invasive, such as sending and receiving e-mail, viewing publicly available, non-proprietary web pages via the browser, or viewing on-line calendars. However, if authentication is successful, the user may use all of the available services of the local computer. One skilled in the art will appreciate that, if authentication fails, one embodiment of the present invention may inhibit the user from using any of the computer's services. In this case, no applets are allowed to be downloaded.

If authentication fails, the browser provides the user with restricted access to the local computer (step 210). In this step, the browser displays icons representative of the services that the user may use, as indicated in the token received from the authentication manager. For example, Figure 5 depicts the browser screen 300 with three icons: icon 502, allowing the user to access an e-mail system; icon 504, allowing the user to use a time management program; and icon 506, allowing the user to browse various web pages on the Internet. Upon selecting one of

the icons 502-506 for the first time, the browser sends a request to the authentication manager for the appropriate service applet, and the authentication manager downloads it to the browser so that the user may use the corresponding service. Subsequent selections of the icon do not cause a download of the service applet; instead, recognizing that a copy has already been downloaded, the browser merely invokes that copy. Also as part of this step, the browser's security level is set to the highest possible setting, resulting in the user's inability to either run programs or access network resources such as files, because the user does not have access to the operating system command interpreter.

In an alternative implementation, all applications are run on servers remote from the local computer. In this situation, all requests for services originating from the local computer include the user's authentication token and pass through the authentication manager, where it is validated (to preclude tampering) and the request as well as the authorization profile (from the authentication file) are forwarded to the appropriate application manager. The application manager then uses this information to decide to what extent to fulfill or respond to the client request.

When the authentication manager determines that an authorized user is present, the authentication token returned to the local computer indicates that the user can utilize all of the available services on the local computer (step 212). In this case, the user has access to a much greater range of capabilities, such as running a variety of programs and accessing numerous local files through their web browser. The user may be granted access to an operating system command interpreter and/or to files via a client application which provides access to directories exported via the well-known Network File System (NFS). Again, the browser displays icons indicating the services to which the user has access. For example, Figure 6 depicts the browser screen 300 displaying four icons: the e-mail icon 502, the calendar icon 504, the browse icon

506, and the file system icon 602. Upon selection of the file system icon 602, an applet facilitating access to the local file system is downloaded from the authentication manager and run.

Although the present invention has been described with reference to a preferred embodiment thereof, those skilled in the art will know of various changes in form and detail which may be made without departing from the spirit and scope of the claimed invention as defined in the appended claims and their full scope of equivalents.

CLAIMS

What is claimed is:

1. A method in a data processing system having a stand-alone computer system and a security node connected via a network, the security node having an authentication manager, the stand-alone computer system having a set of services, the method comprising:

starting up the stand-alone computer system;

inhibiting a user from utilizing the services of the stand-alone computer system responsive to the starting up of the stand-alone computer system;

displaying a browser with a login screen prompting the user for identification;

receiving the identification from the user and sending the identification to the authentication manager;

attempting to authenticate the user by the authentication manager;

determining by the browser whether the authentication manager has authenticated the user;

downloading first code to the stand-alone computer system that facilitates use of a portion of the set of the services of the stand-alone computer system when the user has not been authenticated; and

downloading second code to the stand-alone computer system that facilitates use of the set of the services of the stand-alone computer system when the user has been authenticated.

2. The method of claim 1 wherein the downloading first code includes:

displaying, by the browser, icons representing the portion of the set of services available to the user, and

providing the first code responsive to user selection of the icons.

3. The method of claim 1 wherein the downloading second code includes:

displaying, by the browser, icons representative of the set of services, and

providing the second code responsive to user selection of the icons.

4. The method of claim 1 wherein each of the services of the stand-alone computer system is facilitated by an applet managed by the authentication manager, and wherein the downloading first code includes:

providing from a remote location applets to facilitate use of the portion of the set of services by the user.

5. The method of claim 1 wherein each of the services of the stand-alone computer system is facilitated by an applet managed by the authentication manager, and wherein the downloading second code includes:

downloading applets to facilitate use of the set of services by the user.

6. The method of claim 1 wherein the downloading first code includes:

running the portion of the set of services on the stand-alone computer system.

7. The method of claim 6 wherein the stand-alone computer system has a virtual machine, and wherein the running includes:

running the portion of the set of services on the virtual machine.

8. The method of claim 1 wherein the downloading second code includes:

running the set of services on the stand-alone computer system.

9. The method of claim 8 wherein the stand-alone computer system has a virtual machine, and wherein the running includes:

running the set of services on the virtual machine.

10. A method for performing authentication in a computer system with services, comprising:

receiving an identification of a user;

sending the identification to a remote location for a determination of which among the services the user is authorized to use; and

receiving code that facilitates access to at least one of the services, the user being authorized to use the at least one of the services.

11. The method of claim 10, wherein the computer system includes a browser and wherein the receiving includes:

displaying by the browser a log-on screen to the user requesting the identification.

12. The method of claim 10, wherein the receiving an identification includes:

inhibiting use of the services until it is determined which among the services the user is authorized to use.

13. A method for performing authentication in a data processing system having an authentication server and a computer system with services, the method performed by the authentication server comprising:

receiving an identification of a user of the computer system;

determining which among the services the user is authorized to use; and

sending to the computer system code that facilitates use of at least one of the services that the user is authorized to use.

14. The method of claim 13 wherein the code is contained in an applet, and wherein the sending includes:

sending the applet to the computer system to facilitate use of the at least one of the services that the user is authorized to use.

15. A data processing system with services and a user, comprising:

a security node with an authentication manager configured to receive an identification of the user, configured to authenticate the user based on the identification, and configured to return code that facilitates use of the services when the user has been authenticated; and

a computer system with a browser configured to receive the identification, configured to send the identification to the authentication manager, configured to receive the code returned from the authentication manager, and configured to invoke the code to facilitate use of the services by the user when the user has been authenticated.

16. The data processing system of claim 15 wherein the code is an applet.

17. The data processing system of claim 15 wherein the computer system includes a virtual machine and wherein the browser runs on the virtual machine.

18. A computer-readable medium containing instructions for controlling a computer system to perform a method for performing authentication, the computer system having services, the method comprising:

receiving an identification of a user;

sending the identification to a remote location to determine which among the services the user is authorized to use; and

receiving code that facilitates access to at least one of the services, the user being authorized to use the at least one of the services.

19. The computer-readable medium of claim 18, wherein the computer system includes a browser and wherein the receiving includes:

displaying by the browser a log-on screen to the user requesting the identification.

20. The computer-readable medium of claim 18, wherein the receiving an identification includes:

inhibiting use of the services until it is determined which among the services the user is authorized to use.

21. A computer-readable medium containing instructions for controlling a data processing system to perform a method for performing authentication, the data processing system having an authentication server and a computer system with services, the method performed by the authentication server comprising:

receiving an identification of a user of the computer system;

determining which among the services the user is authorized to use; and

sending to the computer system code that facilitates use of at least one of the services that the user is authorized to use.

22. The computer-readable medium of claim 21 wherein the code is contained in an applet, and wherein the sending includes:

sending the applet to the computer system to facilitate use of the at least one of the services that the user is authorized to use.

23. A data processing system having both a stand-alone computer system and a security node connected via a network, the security node having an authentication manager, the stand-alone computer system having a set of services, the data processing system comprising:

means for starting up the stand-alone computer system;

means for inhibiting a user from utilizing the services of the stand-alone computer system responsive to the starting up of the stand-alone computer system;

means for displaying a browser with a login screen prompting the user for identification;

means for receiving the identification from the user by the browser and sending the identification to the authentication manager;

means for authenticating the user by the authentication manager;

means for determining by the browser whether the authentication manager has authenticated the user;

means for downloading first code to the stand-alone computer system that facilitates use of a portion of the set of the services of the stand-alone computer system when the user has not been authenticated; and

means for downloading second code to the stand-alone computer system that facilitates use of the set of the services of the stand-alone computer system when the user has been authenticated.

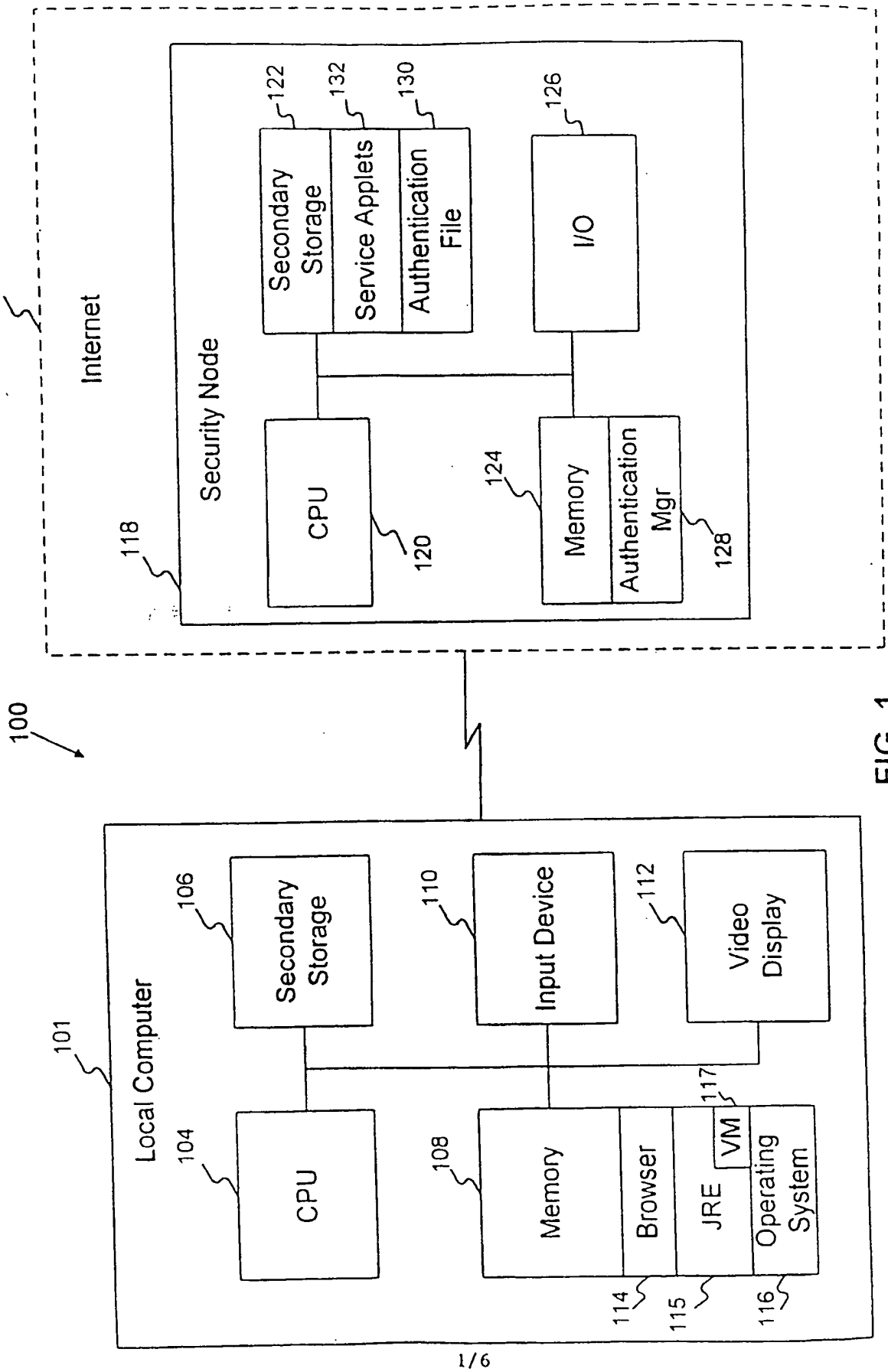

100
102
Internet
Security Node
118
Secondary Storage
122
Service Applets
132
Authentication File
130
I/O
126
CPU
120
Memory
124
Authentication Mgr
128
101
Local Computer
Secondary Storage
106
Input Device
110
Video Display
112
CPU
104
Memory
108
Browser
JRE
VM
117
Operating System
114
115
116

FIG. 1

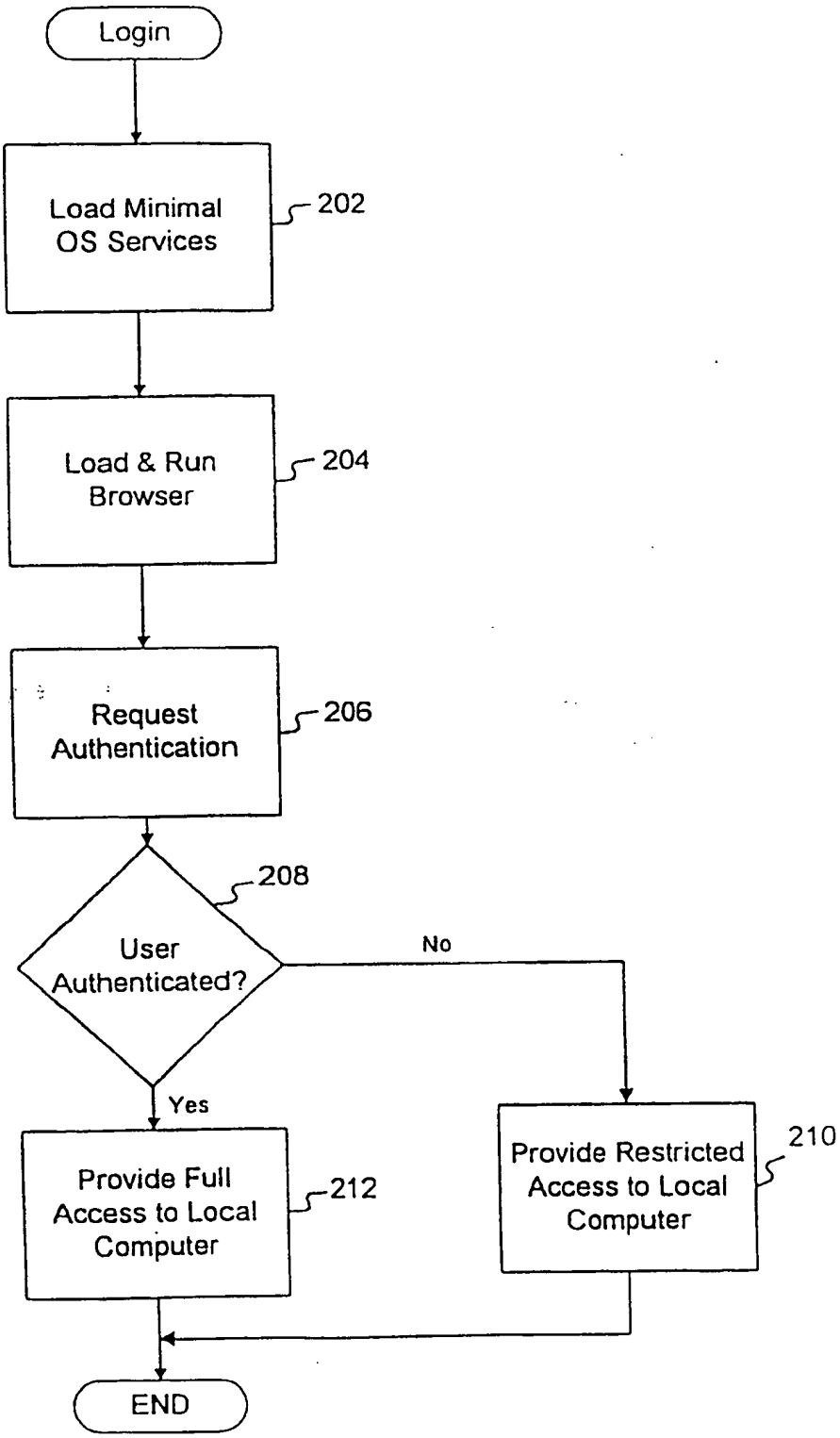

Login
Load Minimal OS Services
202
Load & Run Browser
204
Request Authentication
206
208
User Authenticated?
No
Yes
Provide Full Access to Local Computer
212
Provide Restricted Access to Local Computer
210
END

FIG. 2

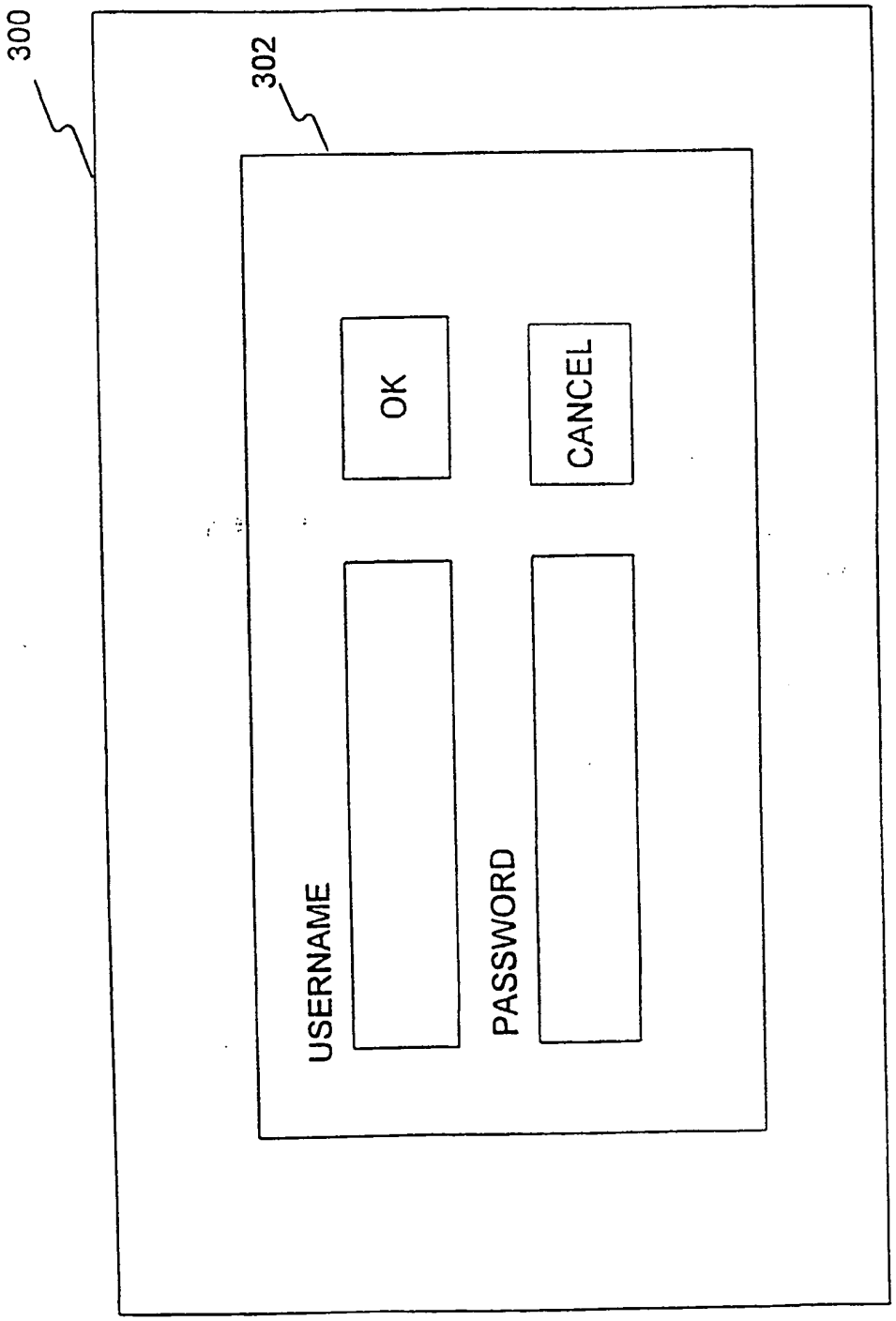


FIG. 3

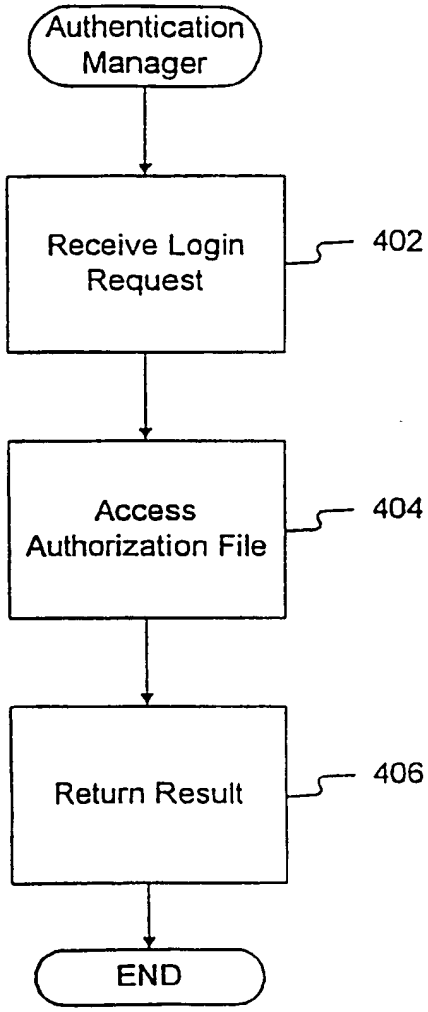

Authentication Manager
Receive Login Request
402
Access Authorization File
404
Return Result
406
END

FIG. 4

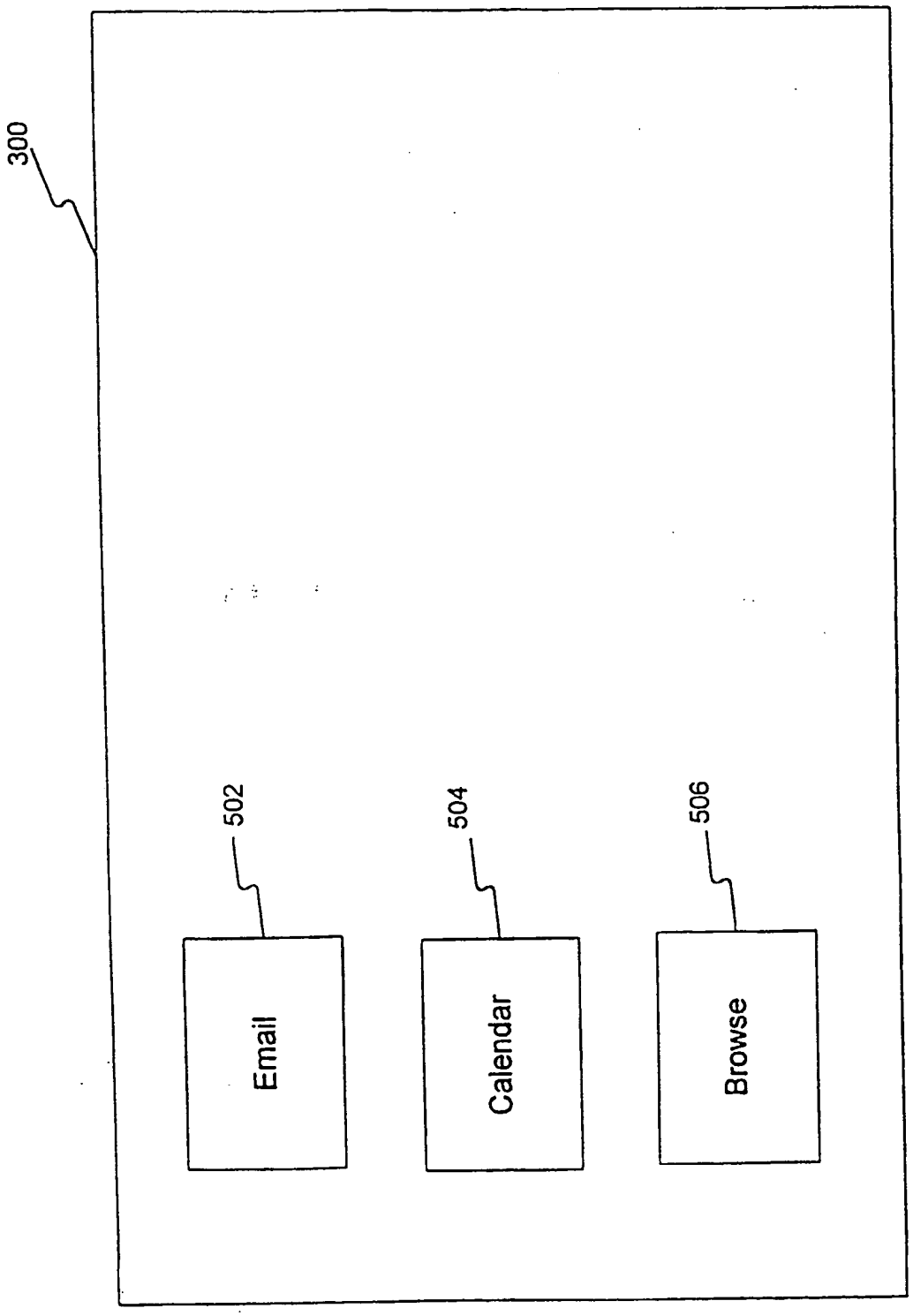


FIG. 5

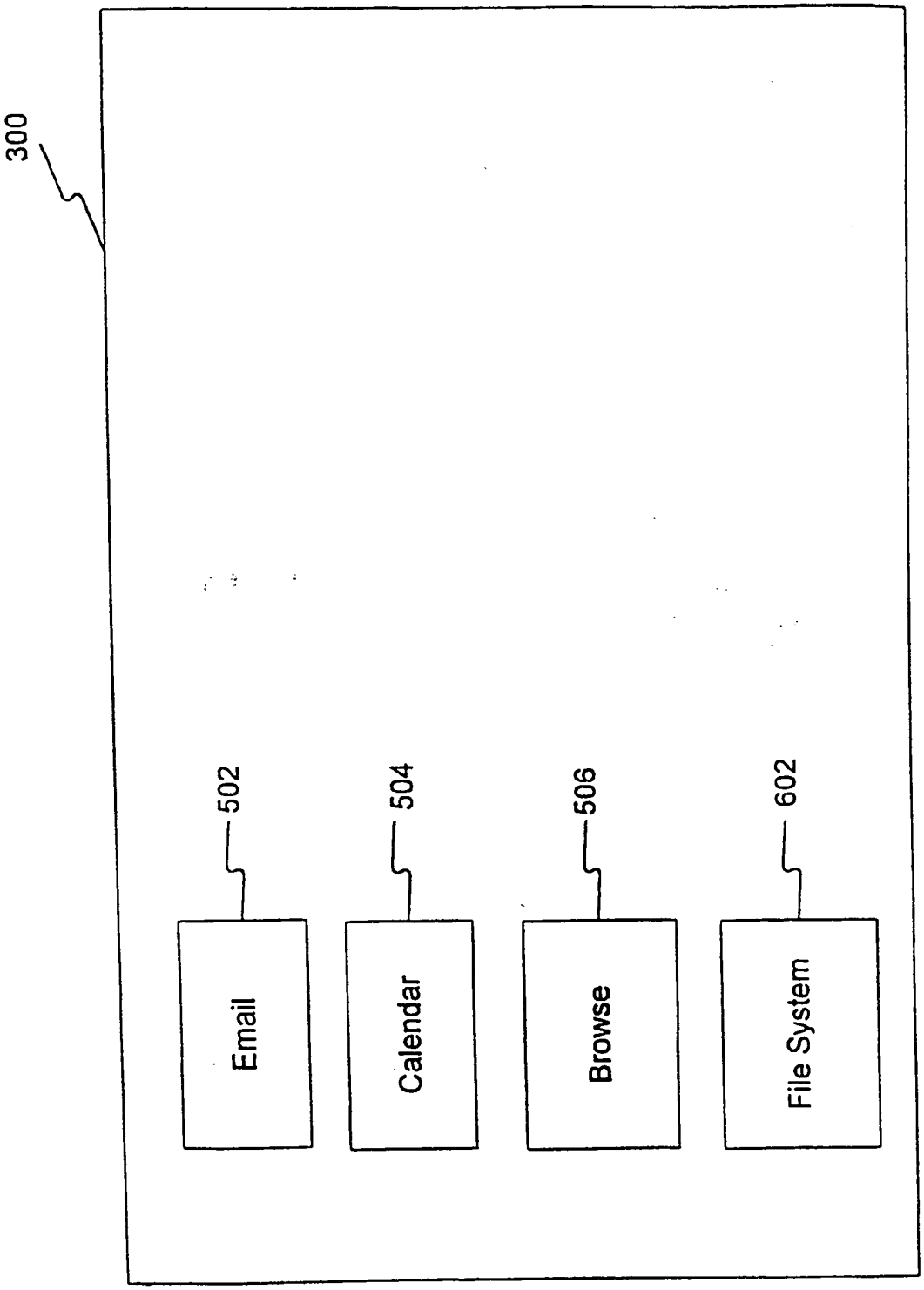


FIG. 6

INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/US 99/01614

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 42041 A (OPEN MARKET INC) 27 December 1996 see figures 1-5 see page 9, line 16 - page 16, line 20	1,6,8, 10-13, 15, 18-21,23
A	EP 0 798 655 A (SUN MICROSYSTEMS INC) 1 October 1997 see figures 1,2,5,6 see page 3, line 43 - page 5, line 48	1-9, 13-17, 21-23

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 1999	28/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Weiss, P

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte .onal Application No
PCT/US 99/01614

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9642041 A	27-12-1996	US 5708780 A	13-01-1998
		US 5812776 A	22-09-1998
		AU 694367 B	16-07-1998
		AU 5936796 A	09-01-1997
		CA 2221506 A	27-12-1996
		EP 0830774 A	25-03-1998
EP 0798655 A	01-10-1997	JP 10069376 A	10-03-1998